CLAIMS:

1. A method of detecting a non-virus component in a virus-protected computer system comprising identifying a software trace of the component and conveying the trace to the computer system as a virus pseudo-signature to allow detection of the component by the system's antivirus software.

2. A method according to claim 1 wherein the trace is conveyed to the computer system as part of an update procedure, whereby additional virus signatures or scanning engines may also be passed to the antivirus software.

3. A method according to claim 1 wherein the component is a hardware device and wherein the software trace is indicative of the presence of the device in the computer system.

4. A method according to claim 3 wherein the software trace is resident in a volatile area of the system's memory.

5. A method according to claim 1 wherein the pseudo-signature is tagged or otherwise marked to distinguish it from authentic virus signatures.

6. A method according to claim 5 wherein the antivirus software is modified so as to react differently to the presence of pseudo and authentic virus signatures.

7. A method according to claim 6 wherein the modification is effected as part of the update procedure.

8. A method according to claim 6 wherein the antivirus software does not attempt to fix, clean, modify or delete the component associated with the pseudo-signature.

9. A method according to claim 6 wherein detection of the pseudo-signature causes an advisory message to be conveyed to a user of the system, advising the user of the presence of the detected component.

10. A method according to claim 6 wherein detection of the pseudo-signature effects a connection to a website providing details of the component concerned.

11. A method of facilitating the detection of a non-virus component in a first virus-protected computer system comprising identifying, on a second computer system, a software trace of the component, and conveying the trace towards an antivirus update source whereby the software trace may be passed, as a virus pseudo-signature, to the first computer system.

12. A method of detecting, in a virus-protected computer system, the presence of a non-virus component comprising receiving a virus pseudo-signature associated with a software trace of the non-virus component, and comparing the pseudo-signature with software traces disposed within the system's memory.

13. A method according to claim 12 wherein, in the event of a match being found, the antivirus software of the system is operative to convey, to a user of the system, an advisory message advising of the presence of the detected component.

14. Apparatus for detecting, in a virus-protected computer system, a non-virus component, comprising a pseudo-signature generation element operative to produce a software trace of the component, and an antivirus support source whereby the software trace may be conveyed, as a virus pseudo-signature, to the computer system.

15. An antivirus update source having a reception element operative to receive software traces indicative of the presence, in a computer system, of a non-virus component, and a dispatch element operative to convey virus signatures to a plurality of computer systems in addition to a pseudo-signature produced in response to the received software trace.

16. An antivirus software element having a virus scanning engine and a signature table containing a plurality of virus signatures, the element also having a distinguishing capability whereby the element responds differently to the detection of virus signatures and virus pseudo-signatures, the latter being indicative of the presence of a non-virus component in a host computer system.

17. Use of an antivirus software element to detect, in a virus-protected computer system, a non-virus component, comprising receiving a virus pseudo-signature generated from a software trace of the component and scanning a host computer system, using the software element, so as to detect the presence of any component therein, having a matching software trace.

18. A method of detecting a non-virus component in a virus-protected computer system comprising identifying a software trace indicative of the presence of a hardware device in the computer system conveying the trace to the computer system as a virus pseudo-signature to allow detection of the device by the system's antivirus software wherein the trace is conveyed to the computer system as part of an update procedure, whereby additional virus signatures or scanning engines may also be passed to the antivirus software.

19. A method according to any one of the preceding claims wherein the pseudo-signature is tagged or otherwise marked to distinguish it from authentic virus signatures.

20. A method according to claim 19 wherein the antivirus software is modified so as to react differently to the presence of pseudo and authentic virus signatures.